



Notebook

Deutsch, English

Benutzerhandbuch / User Manual

# Wireless LAN





## Sie haben...

... technische Fragen oder Probleme?

Wenden Sie sich bitte an:

- unsere Hotline/Help Desk (siehe Help Desk-Liste oder im Internet: "[www.fujitsu-siemens.com/helpdesk](http://www.fujitsu-siemens.com/helpdesk)")
- Ihren zuständigen Vertriebspartner
- Ihre Verkaufsstelle

Weitere Informationen finden Sie auf der Help-Desk-Liste und im Handbuch "Garantie".

Das Handbuch "Garantie" finden Sie auf Ihrem System oder auf der CD/DVD "Drivers & Utilities" oder auf unseren Internetseiten.

Aktuelle Informationen zu unseren Produkten, Tipps, Updates usw. finden Sie im Internet: "[www.fujitsu-siemens.com](http://www.fujitsu-siemens.com)"

## Are there ...

... any technical problems or other questions you wish to discuss?

Please contact:

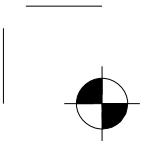
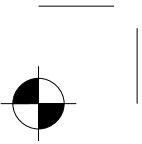
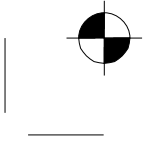
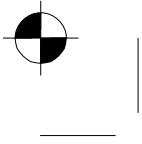
- our Hotline/Help Desk (see the Help Desk list or visit: "[www.fujitsu-siemens.com/helpdesk](http://www.fujitsu-siemens.com/helpdesk)")
- your authorised distributor
- your sales office

Additional information is contained in the Help Desk list and the "Warranty" manual.

The "Warranty" manual can be found on the computer system, on the "Drivers & Utilities" CD/DVD, or on our website.

The latest information on our products, tips, updates etc. can be found on our website: "[www.fujitsu-siemens.com](http://www.fujitsu-siemens.com)"





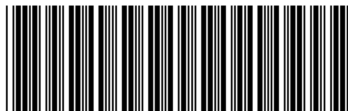


Dieses Handbuch wurde erstellt von / This manual was produced by Xerox Global Services

Herausgegeben von / Published by  
Fujitsu Siemens Computers GmbH  
Ausgabe / Edition 1, September 2007

Bestell-Nr.: / Order no.: 10600902628

Bestell-Nr.: / Order no.: 440 N00558



## Wireless LAN

Benutzerhandbuch / User Manual

Deutsch

English

Microsoft, MS, Windows, Windows Vista sind eingetragene Warenzeichen der Microsoft Corporation.

Alle anderen Warenzeichen sind Warenzeichen oder eingetragene Warenzeichen der jeweiligen Inhaber und werden als geschützt anerkannt.

Alle Rechte vorbehalten, insbesondere (auch auszugsweise) die der Übersetzung, des Nachdrucks, der Wiedergabe durch Kopieren oder ähnliche Verfahren.

Zu widerhandlungen verpflichten zu Schadenersatz.

Alle Rechte vorbehalten, insbesondere für den Fall der Patenterteilung oder GM-Eintragung.

Liefermöglichkeiten und technische Änderungen vorbehalten.

Copyright © Fujitsu Siemens Computers GmbH 2007

Microsoft, MS Windows and Windows Vista are registered trademarks of the Microsoft Corporation.

All other trademarks referenced are trademarks or registered trademarks of their respective owners, whose protected rights are acknowledged.

All rights reserved, including rights of translation, reproduction by printing, copying or similar methods, either in part or in whole.

Non-compliance is subject to compensation for damages.

All rights reserved, including rights created by patent grant or registration of a utility model or design.

Subject to availability and technical modifications.

# Inhalt

|                                                                 |          |
|-----------------------------------------------------------------|----------|
| <b>Wireless LAN allgemein</b>                                   | <b>1</b> |
| Betriebssystem                                                  | 1        |
| Darstellungsmittel                                              | 1        |
| Funknetzwerk nach dem IEEE 802.11-Standard                      | 2        |
| Adhoc-Modus                                                     | 2        |
| Infrastruktur-Modus                                             | 3        |
| Namen für Funknetzwerke (SSID)                                  | 3        |
| 802.11-Netzwerksicherheit                                       | 4        |
| Wired-Equivalent Privacy (WEP) mit vorkonfigurierten Schlüsseln | 4        |
| Wi-Fi Protected Access (WPA) und TKIP-Verschlüsselung           | 5        |
| Wi-Fi Protected Access 2 (WPA2) und AES Verschlüsselung         | 5        |
| 802.1x-Standard                                                 | 5        |
| Extensible Authentication Protocol (EAP)                        | 6        |
| Wichtige Hinweise                                               | 6        |
| Sicherheitshinweise                                             | 6        |
| CE-Kennzeichnung                                                | 7        |
| Wireless LAN unter Windows Vista installieren                   | 7        |

## Inhalt

---

# Wireless LAN allgemein

In Ihrem Gerät ist eine Funknetzwerkkarte integriert. In diesem Benutzerhandbuch werden die Grundlagen für Wireless LAN kurz beschrieben.

## Betriebssystem

Dieses Handbuch ist für das Betriebssystem Windows Vista gültig.

## Darstellungsmittel

|                                                                                     |                                                                                                                                                                                                                                                                                                                                                                                                                 |
|-------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|    | kennzeichnet Hinweise, bei deren Nichtbeachtung Ihre Gesundheit, die Funktionsfähigkeit Ihres Geräts oder die Sicherheit Ihrer Daten gefährdet sind. Die Gewährleistung erlischt, wenn Sie durch Nichtbeachtung dieser Hinweise Defekte am Gerät verursachen                                                                                                                                                    |
|   | kennzeichnet wichtige Informationen für den sachgerechten Umgang mit dem Gerät                                                                                                                                                                                                                                                                                                                                  |
|  | kennzeichnet einen Arbeitsschritt, den Sie ausführen müssen                                                                                                                                                                                                                                                                                                                                                     |
|  | kennzeichnet ein Resultat                                                                                                                                                                                                                                                                                                                                                                                       |
| <b>Diese Schrift</b>                                                                | kennzeichnet Eingaben, die Sie mit der Tastatur in einem Programm-Dialog oder in einer Kommandozeile vornehmen, z. B. Ihr Passwort ( <b>Name123</b> ) oder einen Befehl, um ein Programm zu starten ( <b>start.exe</b> )                                                                                                                                                                                        |
| Diese Schrift                                                                       | kennzeichnet Informationen, die von einem Programm am Bildschirm ausgegeben werden, z. B.: Die Installation ist abgeschlossen!                                                                                                                                                                                                                                                                                  |
| <i>Diese Schrift</i>                                                                | kennzeichnet <ul style="list-style-type: none"> <li>Begriffe und Texte in einer Softwareoberfläche, z. B.: Klicken Sie auf <i>Speichern</i>.</li> <li>Namen von Programmen oder Dateien, z. B. <i>Windows</i> oder <i>setup.exe</i>.</li> </ul>                                                                                                                                                                 |
| "Diese Schrift"                                                                     | kennzeichnet <ul style="list-style-type: none"> <li>Querverweise auf einen anderen Abschnitt z. B. "Sicherheitshinweise"</li> <li>Querverweise auf eine externe Quelle, z. B. eine Webadresse: Lesen Sie weiter auf "www.fujitsu-siemens.com"</li> <li>Namen von CDs, DVDs sowie Bezeichnungen und Titel von anderen Materialien, z. B.: "CD/DVD Drivers &amp; Utilities" oder Handbuch "Sicherheit"</li> </ul> |
|  | kennzeichnet eine Taste auf der Tastatur, z. B.:                                                                                                                                                                                                                                                                           |
| <b>Diese Schrift</b>                                                                | kennzeichnet Begriffe und Texte, die betont oder hervorgehoben werden, z. B.: <b>Gerät nicht ausschalten</b>                                                                                                                                                                                                                                                                                                    |

## Funknetzwerk nach dem IEEE 802.11-Standard

Die integrierte Netzwerkkarte arbeitet nach dem IEEE 802.11-Standard. Als Kommunikationsmedium werden Frequenzen aus den ISM-Frequenzbändern verwendet (ISM, Industrial, Scientific, Medical). Die Funknetzwerkkarte darf ohne Anmeldung und gebührenfrei betrieben werden. Der IEEE 802.11-Standard sieht mehrere Möglichkeiten vor, die ISM-Frequenzbänder zu nutzen:

|                             |                                                                                                                                                     |                           |
|-----------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------|
| IEEE 802.11a                | 5,0-GHz-Band<br>5.150 bis 5.350 MHz; nur im Innenbereich verwendbar<br>5.350 bis 5.725 MHz; ohne Beschränkung im Innen- und Außenbereich verwendbar | 54 Mbit/s                 |
| IEEE 802.11b                | 2,4-GHz-Band<br>2.400 bis 2.483,5 MHz (Ausnahme: Frankreich)                                                                                        | 11 Mbit/s                 |
| IEEE 802.11g                | 2,4-GHz-Band<br>2.400 bis 2.483,5 MHz (Ausnahme: Frankreich)                                                                                        | 54 Mbit/s                 |
| IEEE 802.11n<br>(Draft 2.0) | 2,4-GHz-Band (Ausnahme: Frankreich)<br>5 GHz-Band                                                                                                   | 144 Mbit/s bis 300 Mbit/s |



In Frankreich darf das WLAN-Gerät im Außenbereich nur im Frequenzbereich von 2.454 bis 2.483,5 MHz, mit max. 10 mW verwendet werden.

Die nach 802.11 arbeitenden Funknetzwerke lassen sich leicht mit vorhandenen Ethernet-Netzwerken verbinden. Nach 802.11 arbeitende Funknetzwerkkarten sind bis auf ein paar Zusatzparameter ein System mit einer normalen Ethernet-Karte. Das heißt, dass Sie in einem 802.11-Funknetzwerk alle Protokolle verwenden können, wie in einem kabelgebundenen Ethernet (IP, IPX, NetBIOS, etc.). Der einzige Unterschied ist, dass Sie keine Leitungen zwischen den Computern verlegen müssen. Die Menge aller Wireless-LAN-Stationen, die sich gegenseitig direkt erreichen können, bezeichnet man allgemein als Funkzelle. Der IEEE-Standard bietet zwei Betriebsarten an, den Adhoc-Modus (Peer-to-Peer) und den Infrastruktur-Modus.

Neben der Beschreibung der Modulation und des Data Framing enthält diese Norm ein Authentifizierungs- und Verschlüsselungsverfahren mit der Bezeichnung Wired Equivalent Privacy (WEP). Viele Unternehmen setzen 802.11-Funknetzwerke ein. 802.11-Funknetzwerke findet man jetzt auch in Hotels, auf Flugplätzen und an anderen "Hotspots" mit Zugang zum Internet.

### Adhoc-Modus

Ein Wireless LAN im Adhoc-Modus, auch Peer-to-Peer-Modus genannt, besteht aus einer einzelnen abgeschlossenen Funkzelle. Adhoc-Funknetzwerke entstehen, wenn sich eine Arbeitsgruppe mit ihren Systemen zusammenfindet und diese zum Datenaustausch vernetzen möchte. Systeme können zu einem solchen Netzwerk beliebig hinzukommen und es wieder verlassen.

Damit sich mehrere Adhoc-Funknetzwerke nicht gegenseitig im Funkverkehr behindern, gibt es einen eindeutigen Netzwerknamen, die SSID (Service Set Identifier). Die SSID wird zur Adressierung verwendet, sodass sich ein Datenpaket immer einer bestimmten Funkzelle zuordnen lässt.

Wenn Sie sich in ein bestehendes Funknetzwerk einwählen wollen, benötigen Sie den Netzwerknamen (SSID), den Sie in den Einstellungen für die Netzwerkkarte eintragen. Die Netzwerkkarte sucht dann beim Start nach einem Funknetzwerk mit dieser SSID. Wenn die Netzwerkkarte ein Funknetzwerk gefunden hat, klinkt sie sich in dieses ein und Sie können mit den Systemen in diesem Funknetzwerk kommunizieren. Wenn zwei Funkzellen sehr nah beieinander sind, sollten die Funkkanäle dieser Netzwerke 4 bis 5 Kanäle auseinander liegen. Dies gilt für 802.11b, 802.11g und 802.11n.

## Infrastruktur-Modus

Im Infrastruktur-Modus existiert neben den beweglichen Stationen eine Basisstation, die als AccessPoint bezeichnet wird. Im Infrastruktur-Modus übernimmt der AccessPoint die Funktion eines "Wächters". Im Gegensatz zum Adhoc-Modus muss sich jedes System bei dem AccessPoint anmelden, bevor es Daten in der Funkzelle austauschen darf.

Eine weitere Aufgabe des AccessPoint ist die Verbindung der Funkzelle mit einem kabelgebundenen Ethernet. Da der AccessPoint durch den Zwang zur Anmeldung jederzeit genau weiß, welche Stationen sich auf der Funkseite befinden, kann er exakt entscheiden, welche Daten durchgereicht werden müssen und welche nicht. Diesen Vorgang bezeichnet man auch als Bridging.

Um die Reichweite eines Funknetzwerks zu vergrößern, können mehrere AccessPoints mit der gleichen SSID verwendet werden.

Geht ein System ins Funknetzwerk, sucht es sich unter den erreichbaren AccessPoints den mit dem stärksten Signal aus und meldet sich dort an. Zwei Systeme, die an unterschiedlichen AccessPoints angemeldet sind, kommunizieren so miteinander, auch wenn sie nicht in direkter Funkreichweite sind. Überwacht ein System auch nach der Anmeldung kontinuierlich die Funksituation, kann es erkennen, wie die Signale von einem AccessPoint schwächer und von einer anderen stärker werden und sich für den Benutzer unmerklich ummelden. Diesen Vorgang bezeichnet man als Roaming.

## Namen für Funknetzwerke (SSID)

Jedes Funknetzwerk verfügt über seinen eigenen Namen. Sie können das Funknetzwerk, mit dem Sie sich verbinden wollen, über seinen Namen auswählen. Netzwerknamen ermöglichen den gleichzeitigen Betrieb verschiedener Funknetzwerke nebeneinander in derselben Umgebung, ohne dass diese sich gegenseitig behindern. Wenn beispielsweise das Unternehmen neben Ihnen ebenfalls Funknetzwerke verwendet, möchten Sie sicherstellen, dass Ihr Computer mit dem Netzwerk Ihrer Firma verbunden ist und nicht mit dem anderen, auch wenn sich Ihr Computer im Bereich der benachbarten AccessPoints (Zugangspunkte) liegt. (Wie verhindert wird, dass Fremde sich in Ihr Firmennetzwerk einwählen, ist Gegenstand der nachfolgenden Sicherheitsdiskussion.) Ein Netzwerkname ist einfach eine Folge aus maximal 32 Zeichen, wie z. B. "Bayonne Office" oder "Acme-Marketronics" oder "BE45789". Für Netzwerknamen gilt die Groß- und Kleinschreibung, darum müssen Sie beim Eingeben sorgsam darauf achten. Es steht Ihnen jedoch frei, Namen bereits verfügbarer Netzwerke auszusuchen. Wenn Sie das Netzwerk aus einer Liste auswählen, werden Fehler bei der Namenseingabe vermieden. Die 802.11-Norm legt Netzwerknamen fest wie beispielsweise den "Service Set Identifier" (SSID).

## 802.11-Netzwerksicherheit

Seit dem Aufkommen der Funknetzwerke spielt Sicherheit in weit größerem Maße eine kritische Rolle als früher, aus dem einfachen Grund, weil es Angreifer leichter haben, diese Verbindungen anzupapfen. Bei kabelgebundenen Netzwerken können die meisten Unternehmen den Schutz ihrer Netzwerke gerätetechnisch sichern. Ein Angreifer müsste in die Firmenräume gelangen, um sich in das LAN einzuschalten und den Netzwerkverkehr auszuspionieren.

Alles was man zum Ausspionieren von Daten im Funknetzwerk braucht, ist ein Computer mit einer Funknetzwerkkarte und eine geeignete Stelle draußen auf dem Parkplatz oder im Büro nebenan. Nachfolgend werden einige Voraussetzungen für die sichere Vernetzung beschrieben:

- Ein Benutzer muss vom Netzwerk authentifiziert werden, ehe ihm der Zugriff darauf genehmigt wird, damit das Netzwerk vor Eindringlingen sicher ist.
- Das Netzwerk muss durch den Benutzer authentifiziert sein, ehe er seinem Computer die Verbindung mit dem Netzwerk gestattet. Dadurch wird verhindert, dass ein Funkgerät sich als legitimes Netzwerk ausgibt und Zugriff auf den Computer des Benutzers erhält.
- Die gegenseitige Authentifizierung zwischen Benutzer und Netzwerk muss kryptographisch geschützt werden. Damit wird sichergestellt, dass Sie mit Ihrem gewünschten Netzwerk verbunden werden und nicht mit einem falschen.
- Die Funkverbindung zwischen einem Computer und dem AccessPoint muss so verschlüsselt werden, dass Eindringlinge nicht Zugriff auf Daten erhalten, die als vertraulich gelten.

Für diese Art sicherer Verschlüsselung über ein Funknetzwerk gibt es zwei grundlegende Mechanismen:

- Als WEP-Schlüssel bezeichnete, vorkonfigurierte geheime Angaben. WEP-Schlüssel halten nicht zugelassene Benutzer vom Funknetzwerk fern und verschlüsseln die Daten legitimer Benutzer.
- Authentifizierung mit Hilfe eines 802.1x-Protokolls. Hierbei werden vielfältige zugrunde liegende Authentifizierungsprotokolle für die Zugangskontrolle zum Netzwerk verwendet. Die stärksten dieser Protokolle können gegenseitige Authentifizierung von Benutzer und Netzwerk sichern und können dynamisch Schlüssel zur Verschlüsselung von Funkdaten erzeugen.

## Wired-Equivalent Privacy (WEP) mit vorkonfigurierten Schlüsseln

Mit vorkonfigurierten WEP-Schlüsseln (Wired-Equivalent Privacy) wird dem Client-Computer sowie dem AccessPoint derselbe Geheimschlüssel zugeordnet. Dieser Schlüssel wird dazu verwendet, alle zwischen dem Computer und dem AccessPoint ausgetauschten Daten zu verschlüsseln. Zusätzlich kann der WEP-Schlüssel zur Authentifizierung des Client-Computer am AccessPoint benutzt werden. Falls der Computer nicht nachweisen kann, dass er den WEP-Schlüssel kennt, wird ihm der Zugang zum Netzwerk verwehrt.

- Wenn der AccessPoint einen WEP-Schlüssel für die Authentifizierung erfordert, müssen Sie die Zuordnung zum AccessPoint im Shared-Modus vornehmen. Den Zuordnungsmodus stellen Sie in den Netzwerk-Eigenschaften ein.
- Wenn der AccessPoint keinen WEP-Schlüssel für die Authentifizierung erfordert, wird dies als offener Modus (open) bezeichnet. Den Zuordnungsmodus stellen Sie in den Netzwerk- Eigenschaften ein.

## Wi-Fi Protected Access (WPA) und TKIP-Verschlüsselung

Als Erweiterung der 802.11-Norm umfasst Wi-Fi Protected Access (WPA) eine Reihe von Sicherheitszusätzen über Wired-Equivalent Privacy hinaus.

WPA enthält die Architektur von WEP, bringt jedoch zusätzlichen Schutz durch dynamische Schlüssel, die auf dem Temporal Key Integrity Protocol (TKIP) basieren, und bietet zur Authentifizierung von Nutzern Pre-Shared Keys (PSK) oder Extensible Authentication Protocol (EAP) über IEEE 802.1x an.

TKIP verwendet wie WEP den RC4-Algorithmus für die Verschlüsselung. Der Schlüssel ändert sich temporär - daher auch der Name des Protokolls.

PSK ("vorher vereinbarter Schlüssel") bezeichnet allgemein ein Verschlüsselungsverfahren, bei dem die Schlüssel vor der Kommunikation beiden Teilnehmern bekannt sein müssen, also ein symmetrisches Verfahren.

## Wi-Fi Protected Access 2 (WPA2) und AES Verschlüsselung

Wi-Fi Protected Access 2 (WPA2) und AES Verschlüsselung ist die Implementierung eines Sicherheitsstandards für Funknetzwerke nach den WLAN-Standards IEEE 802.11a, b, g, n und basiert auf dem Advanced Encryption Standard (AES). Er stellt den Nachfolger von WPA dar.

Die Verschlüsselung erfolgt nach dem Advanced Encryption Standard (AES).

Zur Authentifizierung des Clients am Access Point und umgekehrt kann sowohl ein geheimer Text, der "Pre-Shared-Key", als auch ein RADIUS-Server verwendet werden (EAP Authentifizierung).

Die Authentifizierung mit einem Pre-Shared-Key wird oft bei kleinen Installationen, also z.B. im Home-Bereich, benutzt. Diese Variante wird auch als "Personal" bezeichnet.

In größeren Netzen ermöglicht die Verwendung von RADIUS eine zentrale Benutzeradministration inkl. Accounting. Der Access Point leitet in diesem Fall die Authentifizierungsanfrage des Clients an den RADIUS-Server weiter und lässt – je nach Erfolg – den Zugriff zu.

Diese Variante von WPA2 wird oft als "Enterprise" bezeichnet.



WPA-fähige Geräte können in der Regel nicht per Firmware-Update auf den WPA2 Standard gebracht werden. Aus diesem Grunde müssen Sie ihre komplette Wireless LAN Hardware auf WPA2 Hardware austauschen, um diesen Standard nutzen zu können.

## 802.1x-Standard

Das IEEE 802.1x-Protokoll ermöglicht den authentifizierten Zugang zu einem LAN. Diese Norm gilt sowohl für kabellose als auch kabelgebundene Netzwerke. Bei einem Funknetzwerk erfolgt die 802.1x-Authentifizierung, nachdem die 802.11-Zuordnung implementiert ist. Kabelgebundene Netzwerke verwenden die 802.1x-Norm ohne 802.11-Zuordnung.

Das WEP-Protokoll, das vorkonfigurierte Schlüssel verwendet, weist verschiedene Schwächen auf in Bezug auf einfache Verwaltung und Sicherheit. Um diese Probleme zu lösen, hat IEEE eine weitere Norm eingeführt: 802.1x. 802.1x bietet bessere Sicherheit als die vorkonfigurierten WEP-Schlüssel und ist einfach zu handhaben, insbesondere bei großen Netzwerken.

Bei Anwendung vorkonfigurierter WEP-Schlüssel wird der kabellose Client-Computer gegenüber dem Netzwerk authentifiziert. Bei 802.1x wird der Benutzer gegenüber dem Netzwerk mit den Berechtigungsnachweisen authentifiziert (Passwort, Zertifikat oder Token-Karte). Die Authentifizierung wird nicht durch den AccessPoint vorgenommen, sondern vielmehr durch einen zentralen Server. Falls dieser Server das RADIUS-Protokoll benutzt, bezeichnet man ihn als RADIUS-Server.

Bei 802.1x kann ein Benutzer sich bei dem Netzwerk von jedem Computer aus anmelden, und viele AccessPoints können gemeinsam einen einzelnen RADIUS-Server zur Authentifizierung benutzen. Dadurch ist es für den Netzwerkadministrator viel einfacher, den Zugang zum Netzwerk zu kontrollieren.

## Extensible Authentication Protocol (EAP)

802.1x benutzt das Protokoll mit der Bezeichnung EAP (Extensible Authentication Protocol), um die Authentifizierung vorzunehmen. EAP ist kein Authentifizierungsmechanismus an sich, sondern ein gemeinsamer Rahmen für den Transport aktueller Authentifizierungsprotokolle. Der Vorteil des EAP-Protokolls ist, dass der grundlegende EAP-Mechanismus bei der Entwicklung neuer Authentifizierungsprotokolle nicht geändert werden muss.

## Wichtige Hinweise

### Sicherheitshinweise

Die meisten Sicherheitshinweise finden Sie im Handbuch "Sicherheit" oder "Erste Schritte" Ihres Geräts. Einige der wichtigsten Sicherheitshinweise finden Sie im folgenden Text.

- Schalten Sie die Funkkomponente (Bluetooth oder Wireless LAN) am Gerät aus, wenn Sie sich in einem Krankenhaus, einem Operationssaal oder in der Nähe eines medizinischen Elektroniksystems befinden. Die übertragenen Funkwellen können die medizinischen Geräte in ihrer Funktion beeinträchtigen.
- Wie Sie die Funkkomponente ausschalten, ist in dem mit Ihrem Gerät ausgelieferten Handbuch "EasyGuide" beschrieben.
- Halten Sie das Gerät mindestens 20 cm von einem Herzschrittmacher fern, da sonst die ordnungsgemäßen Funktionen des Herzschrittmachers durch Funkwellen beeinträchtigt werden können.
- Die übertragenen Funkwellen können ein unangenehmes Summen in Hörgeräten verursachen.
- Schalten Sie das Gerät aus, wenn Sie sich in einem Flugzeug befinden oder mit dem Auto fahren.
- Bringen Sie das Gerät nicht mit eingeschalteter Funkkomponente in die Nähe entflammbarer Gase oder in eine explosionsgefährdete Umgebung (z. B. Lackiererei), da die übertragenen Funkwellen eine Explosion oder ein Feuer auslösen können.

Das Unternehmen Fujitsu Siemens Computers GmbH ist nicht für Funk- oder Fernsehstörungen verantwortlich, die durch unerlaubte Änderungen an diesem Gerät verursacht wurden. Fujitsu Siemens übernimmt ferner keine Verantwortung für den Ersatz bzw. den Austausch von Anschlussleitungen und Geräten, die nicht von der Fujitsu Siemens Computers GmbH angegeben wurden. Für die Behebung von Störungen, die durch eine derartige unerlaubte Änderung hervorgerufen wurden, und für den Ersatz bzw. den Austausch der Geräte ist allein der Benutzer verantwortlich.

## CE-Kennzeichnung



Dieses Gerät erfüllt in der ausgelieferten Ausführung die Anforderungen der Richtlinie 1999/5/EG des Europäischen Parlamentes und des Rates vom 9. März 1999 über Funkanlagen und Telekommunikationsendeinrichtungen und die gegenseitige Anerkennung der Konformität.

Dieses Gerät darf in Belgien, Bulgarien, Dänemark, Deutschland, Estland, Finnland, Frankreich, Griechenland, Großbritannien, Irland, Island, Italien, Lettland, Liechtenstein, Litauen, Luxemburg, Malta, Niederlanden und Norwegen, Österreich, Polen, Portugal, Rumänien, Schweden, Schweiz, Slowakei, Slowenien, Spanien, Tschechien, Zypern verwendet werden. Aktuelle Information über eventuelle Einschränkungen im Betrieb finden Sie bei der entsprechenden Behörde des jeweiligen Landes. Wenn Ihr Land nicht in der Aufzählung dabei ist, dann wenden Sie sich bitte an die entsprechende Aufsichtsbehörde, ob die Nutzung dieses Produkts in Ihrem Land erlaubt ist.

## Wireless LAN unter Windows Vista installieren

Die Installation von Wireless LAN ist unter dem Betriebssystem Microsoft Windows Vista einfach durchzuführen.

- ▶ Starten Sie die Wireless LAN Installationsroutine von Windows Vista. Diese finden Sie unter *Startsymbol – (Einstellungen) – Netzwerk – Netzwerk- und Freigabecenter*.
- ▶ Folgen Sie den Anweisungen am Bildschirm.
- ▶ Starten Sie das Notebook neu.



Wenn Sie weitere Informationen zu Wireless LAN benötigen, können Sie mit der Taste **F1** die Microsoft Hilfe anzeigen lassen.



# Contents

|                                                              |          |
|--------------------------------------------------------------|----------|
| <b>Wireless LAN (general)</b> .....                          | <b>1</b> |
| Operating system .....                                       | 1        |
| Notational conventions .....                                 | 1        |
| Wireless network as per IEEE 802.11 standard .....           | 2        |
| Ad hoc mode .....                                            | 2        |
| Infrastructure mode .....                                    | 3        |
| Wireless network names (SSID) .....                          | 3        |
| 802.11 network security .....                                | 3        |
| Wired-Equivalent Privacy (WEP) with preconfigured keys ..... | 4        |
| Wi-Fi Protected Access (WPA) and TKIP encryption .....       | 4        |
| Wi-Fi Protected Access 2 (WPA2) and AES encryption .....     | 5        |
| 802.1x standard .....                                        | 5        |
| Extensible Authentication Protocol (EAP) .....               | 5        |
| Important notes .....                                        | 6        |
| Safety instructions .....                                    | 6        |
| CE marking .....                                             | 6        |
| Installing a wireless LAN in Windows Vista .....             | 7        |

## Contents

---

## Wireless LAN (general)

The device purchased includes an integrated wireless network card. This user manual briefly describes the basic principles of wireless LAN.

### Operating system

This user manual is intended for the Windows Vista operating system.

### Notational conventions

|                                                                                     |                                                                                                                                                                                                                                                                                                                                                                                                       |
|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|    | Pay particular attention to text marked with this symbol. Failure to observe this warning will endanger your life, will damage the device or lead to loss of data. The warranty will be invalidated if you cause defects in the device through failure to take notice of this warning                                                                                                                 |
|   | indicates important information that is required to use the device properly.                                                                                                                                                                                                                                                                                                                          |
|  | indicates an activity that must be performed in the order shown                                                                                                                                                                                                                                                                                                                                       |
|  | indicates a result                                                                                                                                                                                                                                                                                                                                                                                    |
| <b>This style</b>                                                                   | flags data entered using the keyboard in a program dialog or command line, e.g. your password ( <b>Name123</b> ) or a command to launch a program ( <b>start.exe</b> )                                                                                                                                                                                                                                |
| <i>This style</i>                                                                   | refers to information displayed by a program on the screen, e.g.:<br>Installation is completed                                                                                                                                                                                                                                                                                                        |
| <i>This style</i>                                                                   | is for <ul style="list-style-type: none"> <li>terms and texts in a software user interface, e.g.: Click <i>Save</i>.</li> <li>names of programs or files, e.g. <i>Windows</i> or <i>setup.exe</i>.</li> </ul>                                                                                                                                                                                         |
| "This style"                                                                        | is for <ul style="list-style-type: none"> <li>cross-references to another section, e.g. "Safety information"</li> <li>cross-references to an external source, e.g. a web address: For more information, go to "www.fujitsu-siemens.com"</li> <li>indicates names of CDs and DVDs as well as names and titles of other materials, e.g.: "CD/DVD Drivers &amp; Utilities" or "Safety" manual</li> </ul> |
|  | refers to a key on the keyboard, e.g.:                                                                                                                                                                                                                                                                             |
| <b>This style</b>                                                                   | flags concepts and text that are emphasised or highlighted, e.g.: <b>Do not switch off device</b>                                                                                                                                                                                                                                                                                                     |

## Wireless network as per IEEE 802.11 standard

The integrated network card operates in accordance with the IEEE 802.11 standard. Frequencies from the ISM frequency bands are used as the communication medium (ISM: Industrial, Scientific, Medical). The wireless network card may be operated free of charge and does not need to be registered. The IEEE 802.11 standard provides several options for using the ISM frequency bands:

|                         |                                                                                                                                           |                          |
|-------------------------|-------------------------------------------------------------------------------------------------------------------------------------------|--------------------------|
| IEEE 802.11a            | 5.0 GHz band<br>5.150 to 5.350 MHz; can only be used indoors<br>5.350 to 5.725 MHz; can be used without restrictions indoors and outdoors | 54 Mbit/s                |
| IEEE 802.11b            | 2.4 GHz band<br>2.400 to 2.4835 MHz (exception: France)                                                                                   | 11 Mbit/s                |
| IEEE 802.11g            | 2.4 GHz band<br>2.400 to 2.4835 MHz (exception: France)                                                                                   | 54 Mbit/s                |
| IEEE 802.11n(Draft 2.0) | 2.4 GHz band (exception: France)<br>5 GHz band                                                                                            | 144 Mbit/s to 300 Mbit/s |



In France, the WLAN device may only be used outdoors in the frequency range 2.454 to 2.4835 MHz with a maximum of 10 mW.

Wireless networks operating in accordance with 802.11 can easily be connected to existing Ethernet networks. With the exception of a few additional parameters, wireless network cards that operate in accordance with 802.11 form one system with a normal Ethernet card. This means that all protocols that can be used in a wired Ethernet network (IP, IPX, NetBIOS, etc...) can also be used in an 802.11 wireless network. The only difference is that there is no need lay cables between the computers. The set of all wireless LAN stations that are in direct range of each other is generally referred to as a cell. The IEEE standard offers two operating modes - the Ad hoc mode (Peer-to-peer) and the Infrastructure mode.

In addition to describing modulation and data framing, this standard includes an authentication and encryption method called Wired Equivalent Privacy (WEP). Many companies are deploying wireless 802.11 networks. 802.11 networks with access to the Internet can now be found in hotels, airports and other "hotspots".

### Ad hoc mode

A wireless LAN in Ad hoc mode, also called Peer-to-peer mode, consists of a single closed cell. Ad hoc wireless networks result when a workgroup comes together with its systems and wants to interconnect these for data exchange. Any number of systems can be added to this type of network and leave it again.

The SSID (Service Set Identifier), a unique network name, is used so that the radio traffic from several ad hoc wireless networks does not create mutual interference. The SSID is used for addressing, so that a data packet can always be assigned to a certain cell.

The network name (SSID) is required to join an existing wireless network, and must be entered in the settings for the network card. The network card then searches for a wireless network with this SSID during start-up. When the network card has found a wireless network, it connects to it and allows communication with the systems in that wireless network. If two cells are very close together, the radio channels of these networks should be 4 to 5 channels apart. This applies to 802.11b, 802.11g and 802.11n.

## Infrastructure mode

In Infrastructure mode, a base station, referred to as an access point, is used in addition to the mobile stations. In Infrastructure mode, the access point assumes the role of a "security guard". In contrast to Ad hoc mode, each system must log on to the access point before it is allowed to exchange data within the cell.

Another task performed by the access point is to connect the cell to a wired Ethernet. Due to the log on requirement, the access point knows at all times exactly which stations are present on the radio side, which means it can decide exactly which data must be passed through and which not. This process is also referred to as bridging.

To increase the range of a wireless network, several access points with the same SSID can be used.

When a system enters the wireless network, it searches among the access points in range for the one with the strongest signal and logs on there. This means that two systems logged on to different access points can communicate with each other, even if they are not within direct radio range. If a system also continuously monitors the radio conditions after logging on, it can detect when the signals from one access point become weaker and those from another become stronger, and can then log on to the stronger one without the user noticing. This procedure is referred to as roaming.

## Wireless network names (SSID)

Each wireless network has its own name. The desired wireless network can be connected to by specifying its name. Network names allow different wireless networks to coexist in the same vicinity without interfering with each other. For example, the company next door to yours may also use wireless networking, so you want to make sure that your computer connects to your company's network, and not that of the neighbour, even though your computer is within range of their access points. (How to prevent intruders from connecting to your company's network is the subject of the security discussion below.) A network name is simply a text sequence up to 32 characters long, such as "Bayonne Office", "Acme-Marketronics" or "BE45789". Network names are case-sensitive, so care must be taken when they entered. However, it is also possible to scan for available networks. This allows you select the network from a list, thereby preventing errors when entering the name. The 802.11 standard defines certain types of network name, for example the "Service Set Identifier" (SSID).

## 802.11 network security

With the advent of wireless networking, security has become a far more critical concern than it was previously, for the simple reason that it is easier for an attacker to eavesdrop on such connections. With wired networking, most organisations can rely on physical

## Wireless LAN (general)

---

security to protect their networks. An attacker would have to get inside a company's offices to be able to connect to the LAN and spy on network traffic.

All it takes to spy on wireless network traffic is a computer fitted with a wireless network card and a suitable spot in the car park outside or the office next door. The following are some of the things that are required to make a wireless network safe:

- In order to make the network safe from intruders, a user must be authenticated by the network before he or she is allowed access.
- The network must be authenticated by the user before the user allows his or her computer to connect to the network. This is to prevent a wireless device posing as a legitimate network from gaining access to the user's computer.
- The mutual authentication between user and the network must be cryptographically protected. This ensures that the user connects to the desired network and not an imposter.
- The wireless connection between a computer and the access point must be encrypted in such a way as to ensure that eavesdroppers cannot access data that is supposed to be private.

There are two basic mechanisms for providing this type of secure encryption over a wireless network:

- Preconfigured secret data, referred to as WEP keys. WEP keys keep unauthorised users off the wireless network and encrypt the data exchanged by legitimate users.
- Authentication using an 802.1x protocol. This uses a variety of underlying authentication protocols to control network access. The strongest of these protocols can provide mutual authentication between the user and the network, and can dynamically create keys to encrypt wireless data.

## Wired-Equivalent Privacy (WEP) with preconfigured keys

With preconfigured WEP (Wired-Equivalent Privacy), both the client computer and access point are assigned the same secret key. This key is used to encrypt all the data exchanged between the computer and the access point. In addition, the WEP key can be used to authenticate the client computer at the access point. Unless the computer can prove it knows the WEP key, it will not be allowed access to the network.

- If the access point requires a WEP key for authentication, then assignment to the access point must be carried out in Shared mode. The association mode is set in the network properties.
- If the access point does not require a WEP key for authentication, this is referred to as Open mode. The association mode is set in the network properties.

## Wi-Fi Protected Access (WPA) and TKIP encryption

As an enhancement to the 802.11 wireless standard, Wi-Fi Protected Access (WPA) encompasses a number of security enhancements over Wired-Equivalent Privacy.

WPA does include the WEP architecture, however it also provides additional protection through dynamic keys, which are based on the Temporal Key Integrity Protocol (TKIP). For user authentication, it offers Pre-Shared Keys (PSK) or the Extensible Authentication Protocol (EAP) via IEEE 802.1x.

TKIP uses the same RC4 algorithm for the encryption as used by WEP. The key changes temporally - hence the name of the protocol.

PSK ("pre-shared key") describes a popular encryption method in which the key is known to both participants prior to the communication, meaning that it is a symmetric method.

## Wi-Fi Protected Access 2 (WPA2) and AES encryption

Wi-Fi Protected Access 2 (WPA2) and AES encryption is the implementation of a security standard for wireless networks according to the WLAN standards IEEE 802.11a, b, g, n, and is based on the Advanced Encryption Standard (AES). It is the replacement for WPA.

The encryption is in accordance with the Advanced Encryption Standard (AES).

Either a secret text string, the "pre-shared key", or a RADIUS server can be used for client authentication at the access point and vice versa (EAP authentication).

Authentication with a pre-shared key is often used for small installations, e.g. for home use. This variant is also referred to as "Personal".

The use of RADIUS allows the possibility of central user administration, including accounting, in larger networks. In this case, the access point transmits the client's authentication request to the RADIUS server and – depending on the outcome – allows access.

This variant of WPA2 is often referred to as "Enterprise".



As a rule, WPA compatible devices cannot be upgraded to the WPA 2 standard using a firmware update. To be able to use this standard, the complete wireless LAN hardware setup must therefore be replaced with WPA2 hardware.

## 802.1x standard

The IEEE 802.1x protocol provides authenticated access to a LAN. This standard applies to both wireless and wired networks. In a wireless network, the 802.1x authentication occurs after the 802.11 association is implemented. Wired networks use the 802.1x standard without any 802.11 association.

The WEP protocol using preconfigured keys has various shortcomings, both in terms of ease of administration and security. To alleviate these problems, the IEEE introduced an additional standard, 802.1x. 802.1x provides better security than preconfigured WEP keys, and is simple to manage, particularly with large networks.

Where preconfigured WEP keys are used, it is the wireless client computer that is authenticated to the network. With 802.1x, it is the user that is authenticated to the network using the user credentials, which may be a password, a certificate, or a token card. The authentication is not performed by the access point, but rather by a central server. If this server uses the RADIUS protocol, it is called a RADIUS server.

With 802.1x, a user can log in to the network from any PC, and multiple access points can share a single RADIUS server for performing the authentication. This makes it much easier for the network administrator to control access to the network.

## Extensible Authentication Protocol (EAP)

802.1x uses the EAP (Extensible Authentication Protocol) protocol to perform authentication. EAP is not an authentication mechanism per se, but rather a common framework for transporting actual authentication protocols. The advantage of EAP is that the basic EAP mechanism does not have to be altered as new authentication protocols are developed.

## Important notes

### Safety instructions

Most of the safety information is contained in the "Safety" or "Getting Started" manual for the device. Some of the most important safety information is outlined below.

- Switch off the radio components (Bluetooth or wireless LAN) on the device if you are in a hospital, an operating theatre or near an electronic medical system. The transmitted radio waves can impair the operation of medical devices.
- The "EasyGuide" manual provided with the device describes how to deactivate the radio components.
- Keep the device at least 20 cm away from pacemakers, as the radio waves may otherwise impair the proper operation of the pacemaker.
- The transmitted radio waves may cause an unpleasant humming in hearing aids.
- Switch off the device when you are in an aircraft or driving in a car.
- Do not bring the device close to flammable gases or into potentially explosive environments (e.g. paint shops) with the radio components switched on, as the transmitted radio waves may cause an explosion or fire.

Fujitsu Siemens Computers GmbH cannot be held responsible for radio or television faults arising from unauthorised modifications made to this device. Furthermore, Fujitsu Siemens shall not be held responsible for replacing and/or exchanging connector cables and devices that have not been specified by Fujitsu Siemens Computers GmbH. The user bears sole responsibility for repairing faults arising from such unauthorised modifications made to a device and for replacing and/or exchanging devices.

### CE marking



This equipment complies with the requirements of Directive 1999/5/EC of the European Parliament and of the Council dated 9 March 1999 concerning radio equipment and telecommunications terminal equipment and the mutual recognition of their conformity.

This device can be used in Belgium, Bulgaria, Denmark, Estonia, Finland, France, Germany, Greece, Great Britain, Ireland, Iceland, Italy, Latvia, Liechtenstein, Lithuania, Luxembourg, Malta, the Netherlands, Norway, Austria, Poland, Portugal, Rumania, Sweden, Switzerland, Slovakia, Slovenia, Spain, Czech Republic, and Cyprus. Please contact the appropriate government office in the respective country for current information on possible operating restrictions. If your country is not included in the list, then please contact the appropriate supervisory authority to establish whether the use of this product is permitted in your country.

## Installing a wireless LAN in Windows Vista

It is simple to install a wireless LAN using the Microsoft Windows Vista operating system.

- ▶ Start the wireless LAN installation routine provided by Windows Vista. This can be found under *Start – (Settings) – Network – Network and Sharing Centre*.
- ▶ Follow the instructions on the screen.
- ▶ Restart the notebook.



If more information relating to wireless LAN is required, this can be obtained by pressing the **F1** key to display the Microsoft Help.

